REMARKS

Claims 1, 18-21, 72-84 and 109-131 are pending in this patent application. Reconsideration of the rejections in view of the remarks below is requested.

This is the **fifth** Office Action on the merits for this application, the first being issued about 3-1/2 years ago. Applicant submits that this application has been thoroughly examined and expects immediate allowance of this application. If there is anything that is preventing allowance of this application, Applicant kindly urges the Examiner to contact the undersigned immediately to work out how the application can be put into form for allowance. Applicant is concerned about such extended and piecemeal examination at least because it significantly impacts Applicant's patent term.

Rejection under 35 U.S.C. §112

The Office Action rejected claims 1, 18-21, 72-78 and 116-129 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to comply with the written description requirement. Applicant respectfully traverses.

With respect to claims 1 and 73, for example, Applicant submits those claims clearly and consistently provide that, in response to the recited digital signing, the recipient is permitted to utilize the recited public key and that prior to the digital signing, utilization of the public key is denied. Nevertheless, the Office Action asserts that the specification does not "disclose denying access to the public key instead [disclosing that] no one who has not signed the system rules agreement may possess a copy of it (page 36 lines 5-15)."

Respectfully, the application as filed clearly discloses examples of denying access to the public key or more generally denying utilization of the public key. In one example embodiment, the public key is not distributed to the recipient unless the recipient performs the digital signing. See, e.g., Applicant's specification, page 35, lines 24-33. Therefore, the user is denied access to, or more generally denied utilization of, the public key prior to the digital signing is performed. In another example embodiment, a secure device contains the public key but the recipient cannot utilize the public key, i.e., the public key cannot be obtained from the secure device, until the recipient performs the digital signing. See, e.g., claim 18. Again, the user is denied utilization of the public key prior to the digital signing is performed.

Therefore, for at least the above reasons, Applicant respectfully submits that the rejection under 35 U.S.C. §112 of claims 1, 18-21, 72-78 and 116-129 should be withdrawn and the claims be allowed.

Rejection under 35 U.S.C. §103 in view of Muftic, Ryder and Miller

The Office Action rejected claims 1, 21, 72, 73, 77, 78, 116-120, 129 and 130 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,745,574 ("Muftic") in view of U.S. Patent No. 4,953,209 ("Ryder") further in view of U.S. Patent No. 5,852,666 ("Miller"). Applicant respectfully traverses the rejection, without prejudice.

Muftic discloses a system that may have the ability to provide efficient key management and distribution in a secure manner by several different ways, more effective than existing models, and in a manner which protects public keys from tampering. (Muftic, col. 4, line 65 to col. 5, line 2). Muftic discloses that certification begins with a message sent from the station desiring certification to the certifying authority or by receiving that notification in any other way. Typically, this is done in a Certificate_Signature_Request message. The format of the Certificate_Signature_Request includes a certificate filled in with at least the public key which the requesting entity desires to have certified. The submission may be self-signed using the requestor's private key and transmitted to the CA for signature. When the CA receives the Certificate_Signature_Request, the information contained therein is validated in accordance with the policies established by a policy certification authority, and if the information is correct, the certifying authority issues a Certificate_Signature_Reply message returning to the requesting entity a signed certificate. When the requesting entity receives the Certificate_Signature_Reply message, it undertakes a Receive_Certificate process which verifies the signature on the certificate and stores it in a local certificate data base after verifying that the public key contained in the certificate corresponds to the entity's private key. (Muftic, col. 11, lines 29-53). To verify the signature, the requesting entity has the public key of the certification authority. (Muftic, col. 12, lines 23-43).

As acknowledged in the Office Action, the cited portions of Muftic fail to at least disclose or teach a recipient digitally signing a message, by which said recipient agrees to rules, and in response to said digital signing, permitting said recipient to utilize said public key and prior to said digital signing, denying utilization of said public key.

However, the Office Action states that "Muftic discloses providing the recipient with at least one message containing the rules of the system including a rule regarding maintaining secrecy of public key in (column 10 lines 52-57)." Applicant respectfully disagrees.

Applicant submits that the cited portions of Muftic also fail to disclose or teach agreeing to rules including a rule regarding maintaining secrecy of the public key.

In that citation (col. 10, lines 52-57), Muftic merely discloses the nature of a certificate from a certifying authority and the process of requesting such a certificate from the certifying authority. As discussed above, the certificates are requested by forwarding a public key and thus the certificate requestor already has access to or use of a public key. There is no disclosure in the cited portions of Muftic of a message containing rules including a rule regarding maintaining secrecy of the public key. There is simply no teaching in Muftic of a recipient of a public key maintaining the public key secret, let alone a recipient agreeing to rules including a rule regarding maintaining secrecy of the public key. As noted above, the public key in Muftic is freely available to users and there is no indication in the cited portions of Muftic of an obligation of a user to keep the public key secret, let alone a user agreeing to rules including a rule maintaining secrecy of the public key.

Thus, the cited portions of Muftic fail to at least disclose or render obvious, *inter alia*, digitally signing said at least one message, by which said recipient agrees to rules including a rule regarding maintaining secrecy of the public key, and in response to said digital signing, permitting said recipient to utilize said public key and prior to said digital signing, denying utilization of said public key as recited in claim 1 or in response to said recipient digitally signing said message, by which said recipient agrees to rules including a rule regarding maintaining secrecy of the public key, permitting said recipient to utilize said public key and prior to said recipient digitally signing said message, denying use of said public key as recited in claim 73.

Further, assuming *arguendo* that the cited portions of Ryder are properly combinable with the cited portions of Muftic (which Applicant does not concede and disagrees that they are), Applicant submits that the cited portions of Ryder fail to overcome the shortcomings of the cited portions of Muftic, or vice versa. Ryder merely discloses a system for electronically transmitting data objects such as computer programs with a means for verifying that the computer program was actually received and the terms and conditions of its use accepted by the receiver is presented. (Ryder, Abstract).

The cited portions of Ryder simply have no disclosure or teaching regarding a public key. Accordingly, the cited portions of Ryder simply have no disclosure or teaching regarding in response to a digital signing, permitting a recipient to utilize a public key and prior to the digital signing, denying utilization of a public key. The cited portions of Ryder further have no disclosure or teaching regarding rules including a rule regarding maintaining

secrecy of the public key, let alone digitally signing a message including the rules, by which said recipient agrees to the rules. Ryder does not even include the words secret or confidential.

Further, assuming *arguendo* that the cited portions of Miller are properly combinable with the cited portions of Muftic and Ryder (which Applicant does not concede and disagrees that they are), Applicant submits that the cited portions of Miller fail to overcome the shortcomings of the cited portions of Muftic and Ryder, or vice versa.

Miller discloses a system providing capability security for distributed object systems. The cited portions of Miller disclose a message 161 that includes an object reference (i.e., the public key) of the referenced object and the location (process and machine) of the referenced object. Before issuing this message 161, the sending object encrypts this information using the encryption method E() 252 and the public key of the intended object. The intended object then decrypts the message to obtain the object reference and the location of the referenced object.

However, these cited portions of Miller simply have no disclosure or teaching regarding in response to a digital signing of a message, permitting a recipient to utilize a public key and prior to the digital signing, denying utilization of a public key. Rather, the cited portions of Miller merely disclose an object decrypting a message containing an object reference.

Further, the cited portions of Miller have no disclosure or teaching regarding a rule regarding maintaining secrecy of the public key, let alone digitally signing a message containing such a rule, by which said recipient agrees to the rule. The cited portions of Miller do not address a rule regarding maintaining secrecy of a public key. Rather, those cited portions of Miller merely disclose encrypting the object reference for supply to an intended object so as to prevent outsiders from being able to access the object reference during transmission and to help ensure the intended object receives the message with the object reference. However, that does not disclose a rule to be agreed by a recipient that a public key is to be maintained in secret. Moreover, those cited portions of Miller do not disclose a message containing such a rule and a recipient digitally signing a message containing such a rule, by which the recipient agrees to such a rule. Rather, the cited portions of Miller merely disclose a message containing an object reference and a location of the referenced object referenced; there is no rule regarding maintaining secrecy of a public key in that message. Moreover, there is no indication in the cited portions of Miller that the intended object

digitally signs the message containing such a rule or that the intended object has an obligation to maintain a public key secret.

Therefore, for at least the above reasons, the cited portions of Muftic, Ryder or Miller, alone or in proper combination, fail to disclose or render obvious all the features recited by claims 1 and 73. Claims 21, 72, 77, 78, 116-120, 129 and 130 depend from claims 1 and 73 respectively and are thus patentable at least for the same reasons as claims 1 and 73 respectively, and for the additional features recited therein. As a result, Applicant respectfully submits that the rejection under 35 U.S.C. §103(a) of claims 1, 21, 72, 73, 77, 78, 116-120, 129 and 130 based on Muftic, Ryder and Miller should be withdrawn and the claims be allowed.

Rejection under 35 U.S.C. §103 in view of Muftic, Ryder, Miller and Curry

The Office Action rejected claims 18, 20, 74, 121-128 and 131 under 35 U.S.C. §103(a) as being obvious in view of Muftic, Ryder, Miller and further in view of U.S. Patent No. 5,940,510 to Curry et al. ("Curry"). Applicant respectfully traverses the rejection, without prejudice.

For at least the reasons discussed above, claims 1 and 73 are patentable over the cited portions of Muftic, Ryder and Miller.

Further, assuming *arguendo* that Curry is properly combinable with the cited portions of Muftic, Ryder and Miller (which Applicant does not concede and disagrees that they are), the cited portions of Curry do not overcome the shortcomings of the cited portions of Muftic, Ryder and Miller, or vice versa. Curry merely disclose a secure device that may have the ability to store or create a private/public key set, whereby the private key never leaves the secure device and is not revealed under almost any circumstance. (Curry, col. 4, lines 49-52).

Therefore, the cited portions of Curry alone or in combination with the cited portions of Muftic, Ryder and Miller, fail to disclose or render obvious, *inter alia,* in response to said digital signing, permitting said recipient to utilize said public key and prior to said digital signing, denying utilization of said public key as recited in claim 1 or *inter alia,* in response to said recipient digitally signing said message, by which said recipient agrees to said rules, permitting said recipient to utilize said public key and prior to said recipient digitally signing said message, denying use of said public key as recited in claim 73.

Claims 18, 20, 74, 121-125, 127, 128 and 131 depend from claims 1 and 73 respectively and are, therefore, patentable over Muftic, Ryder, Miller and Curry for at least

the same reasons as provided above in respect of claims 1 and 73 respectively above, and for the additional features recited therein.

Therefore, for at least the above reasons, the cited portions of Muftic, Ryder, Miller, or Curry, alone or in proper combination, fail to disclose or render obvious all the features recited by claims 18, 20, 74, 121-128 and 131. As a result, Applicant respectfully submits that the rejection of claims 18, 20, 74, 121-128 and 131 under 35 U.S.C. §103(a) in view of Muftic, Ryder, Miller and Curry should be withdrawn and the claims be allowed.

Rejection under 35 U.S.C. §103 in view of Muftic, Ryder, Miller and Curry

The Office Action rejected claims 79, 80, 83, 84 and 109-115 under 35 U.S.C. §103(a) as being obvious in view of Muftic, Ryder, Miller and further in view of Curry. Applicant respectfully traverses the rejection, without prejudice.

Assuming *arguendo* that the cited portions of Muftic, Ryder, Miller and Curry are properly combinable (which Applicant does not concede and disagrees that they are), Applicant submits that the cited portions of Muftic, Ryder, Miller and Curry fail to disclose or render obvious a method of enforcing a security policy in a cryptographic system comprising, *inter alia*, providing a recipient with a message containing rules of said system and with a secure device containing an inactive form of said public key, wherein said public key cannot be obtained from said device, and in response to said recipient digitally signing said message, activating said public key in said secure device, as recited in claim 79.

Applicant respectfully submits that the citations to col. 15, lines 32-43 and col. 12, lines 60-64 of Muftic are inapposite to claim 79. In those citations, Muftic merely discloses a certifying authority re-signing a certificate, which involves a certifying authority generating a new key pair for generating the certificate. Those citations fail to provide any disclosure or teaching regarding an inactive form of a public key, let alone about a secure device containing the inactive form of the public key and from which the public key cannot be obtained (except in response to said recipient digitally signing said message, which activates the public key) or about activating the public key.

Further, as discussed above, Ryder merely discloses a system for electronically transmitting data objects such as computer programs with a means for verifying that the computer program was actually received and the terms and conditions of its use accepted by the receiver is presented.. The cited portions of Ryder simply have no disclosure or teaching regarding a public key. Accordingly, the cited portions of Ryder simply have no disclosure or teaching regarding an inactive form of a public key, let alone about a secure device

containing the inactive form of the public key and from which the public key cannot be obtained (except in response to said recipient digitally signing said message, which activates the public key) or about activating the public key.

The Miller reference merely discloses a system providing capability security for distributed object systems. The cited portions of Miller disclose a message 161 that includes an object reference (i.e., the public key) of the referenced object and the location (process and machine) of the referenced object. Before issuing this message 161, the sending object encrypts this information using the encryption method E() 252 and the public key of the intended object. The intended object then decrypts the message to obtain the object reference and the location of the referenced object.

However, these cited portions of Miller simply have no disclosure or teaching regarding an inactive form of a public key, let alone about a secure device containing the inactive form of the public key and from which the public key cannot be obtained (except in response to said recipient digitally signing said message, which activates the public key) or about activating the public key. There is simply no indication of any public key in Miller having an inactive form. There is simply no indication in Miller of any secure device containing a public key, let alone an inactive form of the public key. Rather, the cited portions of Miller merely disclose an object decrypting a message containing an object reference.

Further, Applicant submits that the cited portions of Curry do not overcome the shortcomings of the cited portions of Muftic, Ryder and Miller, or vice versa. Curry merely disclose a secure device that may have the ability to store or create a private/public key set, whereby the private key never leaves the secure device and is not revealed under almost any circumstance. (Curry, col. 4, lines 49-52). Thus, the cited portions of Curry simply have no disclosure or teaching regarding an inactive form of a public key, let alone about a secure device containing the inactive form of the public key and from which the public key cannot be obtained (except in response to said recipient digitally signing said message, which activates the public key) or about activating the public key.

Thus, Applicant submits that the cited portions of Muftic, Ryder, Miller, or Curry, alone or in proper combination fail to disclose or render obvious claim 79.

Claims 80, 83, 84 and 109-115 depend from claim 79 and are thus patentable at least for the same reasons as claim 79, and for the additional features recited therein.

Therefore, for at least the above reasons, the cited portions of Muftic, Ryder, Miller and Curry fail to disclose or render obvious all the features recited by claims 79, 80, 83, 84 and 109-115. As a result, Applicant respectfully submits that the rejection of claims 79, 80, 83, 84 and 109-115 under 35 U.S.C. §103(a) in view of Muftic, Ryder, Miller and Curry should be withdrawn and the claims be allowed.

All rejections having been addressed, it is respectfully submitted that the present application is in condition for allowance. If questions relating to patentability remain, the Examiner is invited to contact the undersigned to discuss them.

Should any fees be due, please charge them to our deposit account no. 03-3975, under our order no. 061047/0264493. The Commissioner for Patents is also authorized to credit any over payments to the above-referenced deposit account.

Respectfully submitted,
PILLSBURY WINTHROP SHAW PITTMAN LLP

Jean-Paul G. Hoffman
Reg. No. 42,663
Tel. No. 703-770-7794
Fax No. 703-770-7901

P. O. Box 10500
McLean, VA 22102
(703) 770-7900